(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 juillet 2004 (15.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/059493 A2

(51) Classification internationale des brevets[7] : G06F 12/14

(21) Numéro de la demande internationale :
PCT/FR2003/003904

(22) Date de dépôt international :
23 décembre 2003 (23.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/16933 24 décembre 2002 (24.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **TRUSTED LOGIC** [FR/FR]; 5, rue du Bailliage, F-78000 Versailles (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **HAMEAU, Patrice** [FR/FR]; 18, rue de Belle Feuille, F-92100 Boulogne Billancourt (FR). **LE METAYER, Daniel** [FR/FR]; 23, rue de la Celle, F-78150 Le Chesnay (FR). **MESNIL, Cédric** [FR/FR]; 25, avenue du Val d'Arcy, F-78340 Les Clayes sous Bois (FR).

(74) Mandataire : **DE SAINT PALAIS, Arnaud**; Cabinet Moutard, 35, rue de la Paroisse, F-78000 Versailles (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** METHOD OF SECURING COMPUTER SYSTEMS BY MEANS OF SOFTWARE CONTAINMENT

(54) **Titre :** PROCEDE DE SECURISATION DES SYSTEMES INFORMATIQUES PAR CONFINEMENT LOGICIEL

(57) **Abstract:** The invention relates to a method of securing computer systems involving the logical containment of data. More specifically, the invention relates to a method of securing computer systems, which offers the possibility of executing codes that manipulate data which must be processed separately. The inventive method essentially involves the use of the following: (i) a memory manager for managing memory allocation units which can be typically a fixed-size page or a variable-size block, and (ii) memory allocation owners and requesters which can be typically user applications of the operating system of the computer system or the actual operating system. The system involves the separation of the aforementioned data by the owner and the encryption of same with a dedicated key.

(57) **Abrégé :** La présente invention concerne la sécurisation des systèmes informatiques par confinement logique de données. Elle a plus particulièrement pour objet la sécurisation des systèmes informatiques offrant la possibilité d'exécution de codes manipulant des données qui doivent être traitées séparément. Elle fait essentiellement intervenir - un gestionnaire de mémoire gérant des unités d'allocation mémoire qui peuvent être typiquement une page de taille fixe ou un bloc de taille variable, - des possesseurs et des demandeurs d'allocation mémoire pouvant être typiquement des applications de l'utilisateur du système d'exploitation du système informatique ou le système d'exploitation lui-même. Elle exploite la séparation desdites données par possesseur et leur chiffrement avec une clé dédiée.

WO 2004/059493 A2

PROCEDE DE SECURISATION DES SYSTEMES INFORMATIQUES PAR CONFINEMENT LOGICIEL.

La présente invention concerne la sécurisation des systèmes informatiques par confinement logique de données.

Elle a plus particulièrement pour objet la sécurisation des systèmes informatiques offrant la possibilité d'exécution de codes manipulant des données qui doivent être traitées séparément. Cette séparation est généralement dictée par des besoins de sécurité. A titre d'exemple, les données du système d'exploitation qui conditionnent le bon fonctionnement de la plate-forme ne doivent pas pouvoir être modifiées par une application quelconque. De même, dans les systèmes permettant l'exécution d'applications multiples, les données d'une application doivent généralement être protégées des autres applications.

Ces besoins prennent dans certains cas un caractère critique ; on peut penser par exemple, et de manière non limitative, aux systèmes embarqués multi-applicatifs du type cartes à puce, terminaux de paiement, assistants digitaux, ou téléphones portatifs, surtout lorsque ces systèmes embarqués permettent le télé-chargement d'applications. En effet, ces applications téléchargées peuvent provenir de sites multiples, qui offrent des garanties de confiance très variées.

D'une façon générale, on sait que la plupart des solutions généralement adoptées pour répondre à ce besoin de séparation desdites données de systèmes d'exploitation et d'applications repose sur l'utilisation de mécanismes proposés par le matériel. Typiquement, des unités (physiques) de gestion de mémoire ("MMU, ou Memory Management Unit") associent des espaces physiques à des applications et les protègent contre des accès provenant d'autres applications. Cependant, cette solution, quand elle est disponible, n'est pas très souple et s'associe difficilement aux systèmes d'allocation dynamique de données (le nombre d'espaces physiques étant fixe), spécialement dans le cas des systèmes embarqués disposant de peu de ressources et soumis à de fortes contraintes de sécurité.

La présente invention a donc plus particulièrement pour but de palier à ces inconvénients.

Elle propose, à cet effet, de rendre plus flexible la sécurisation des données et de l'étendre au cas d'allocation dynamique de mémoire.

Elle fait essentiellement intervenir :

- au moins un gestionnaire de mémoire gérant des unités d'allocation mémoire qui peuvent être typiquement une page de taille fixe ou un bloc de taille variable,
- au moins des possesseurs et des demandeurs d'allocation mémoire pouvant être typiquement des applications de l'utilisateur du système d'exploitation du système informatique ou le système d'exploitation lui-même.

Selon l'invention, le procédé de sécurisation d'un système informatique par confinement logique de données comprend la séparation desdites données par possesseur et leur chiffrement avec une clé dédiée ; ce processus de

séparation et de chiffrement s'effectue grâce à un mode opératoire comprenant les étapes suivantes :

- une allocation de mémoire réalisée par un gestionnaire de mémoire à la demande d'un autre composant du système d'exploitation qui transmet audit gestionnaire de mémoire l'identité du demandeur. Ce demandeur deviendra le possesseur de la mémoire allouée. La transmission de l'identité du demandeur peut se faire soit par la gestion d'un contexte courant, soit par le passage de paramètres aux fonctions du gestionnaire de mémoire ;
- un contrôle par le susdit gestionnaire de mémoire de l'ensemble des unités d'allocation mémoire, chacune étant associée à un possesseur de l'unité d'allocation mémoire. Chaque unité d'allocation mémoire ne peut avoir qu'un et un seul possesseur ; néanmoins plusieurs unités d'allocation mémoire peuvent avoir le même possesseur ;
- un chiffrement des données de chaque possesseur à l'aide d'une clé associée à ce possesseur ;
- éventuellement une utilisation par le gestionnaire de mémoire d'un secret associé à chaque possesseur. Ce secret peut typiquement être fourni au gestionnaire de mémoire par le système d'exploitation au moment de l'introduction du possesseur dans le système ou à chaque accès à une unité d'allocation mémoire ;
- éventuellement une utilisation par le gestionnaire de mémoire d'une clé pour chaque possesseur. Cette clé peut par exemple être dérivée d'un secret associé au possesseur et une clé dite "maître" à laquelle seul le gestionnaire de mémoire a accès ;
- une vérification par le gestionnaire de mémoire, pour chaque demande d'accès à une unité d'allocation mémoire, de l'identité du demandeur ; si cette identité n'est pas identique à celle du possesseur de ladite unité d'allocation mémoire, alors l'accès à l'unité d'allocation mémoire est refusé par le gestionnaire de mémoire ;

- une réalisation par le gestionnaire de mémoire du chiffrement (dans le cas d'une demande d'écriture) ou du déchiffrement (dans le cas d'une demande de lecture) des données concernées avec la clé associée au possesseur, cette clé pouvant être recalculée par le gestionnaire de mémoire.

Ainsi, les données des différents possesseurs étant chiffrées de manière automatique, par un secret que seul le gestionnaire de mémoire connaît, il est impossible pour une application d'avoir accès aux données d'un autre possesseur.

Deux situations peuvent se présenter lorsqu'un tiers tente d'accéder à une unité d'allocation mémoire qui ne lui appartient pas :

- cette tentative peut être déclenchée par l'intermédiaire du gestionnaire de mémoire : dans ce cas, le contrôle effectué par le gestionnaire de mémoire conduit automatiquement au rejet de la demande ;
- cette tentative peut être déclenchée de manière illicite, sans passer par l'intermédiaire du gestionnaire de mémoire, par accès direct à la mémoire physique, dans le cas où les vérifications effectuées par le matériel ne suffisent pas à écarter cette possibilité : le tiers pourra alors effectuer une lecture, mais, ne disposant pas de la clé de déchiffrement, il obtiendra des données inutilisables.

A partir du moment où la clé maître est mémorisée dans une zone protégée, la confidentialité des données est donc préservée dans les deux cas.

Avantageusement, le procédé selon l'invention ne dépend pas du fait que l'unité d'allocation mémoire soit une page logique de taille fixe ou un bloc de taille variable. Dans le cas où l'unité d'allocation est la page, le procédé se raffinera de la façon suivante : lorsque le gestionnaire de mémoire reçoit une demande d'allocation d'un bloc pour le compte d'un possesseur, il recherche d'abord une page ayant le même possesseur ; ainsi, tous les blocs alloués par

un possesseur d'unité d'allocation mémoire se trouvent regroupés dans une ou plusieurs pages dédiées.

Le procédé selon l'invention pourra être amélioré de plusieurs manières (non exclusives) :

- Au lieu d'associer une clé unique à un possesseur donné, le gestionnaire de mémoire peut associer une clé à chaque ensemble possesseur et unité d'allocation mémoire. Cette amélioration a deux avantages : d'une part, elle réduit les probabilités de découverte des clés utilisées (en cas d'attaque cryptographique) puisque chaque clé sera utilisée moins souvent ; d'autre part, elle réduit les risques en cas de découverte d'une clé puisque seule l'unité d'allocation mémoire associée sera mise en danger.

- Le gestionnaire de mémoire peut également intégrer dans chaque unité de mémoire une zone permettant d'en vérifier l'intégrité, par exemple à partir d'un simple "checksum" (somme des contrôles) signé ou d'un algorithme cryptographique. La donnée contenue dans cette zone est mise à jour par le gestionnaire de mémoire à chaque accès en écriture à l'unité. Elle peut être utilisée par le gestionnaire de mémoire à des fins de vérification, soit systématiquement à chaque accès à l'unité, soit de façon périodique. La vérification consiste simplement, avant l'accès demandé, à recalculer la donnée d'intégrité à partir du contenu de l'unité (données en clair) et à la comparer à la donnée contenue dans la zone d'intégrité. Une modification intempestive ou illicite du contenu de l'unité pourra alors être détectée, ce qui renforcera la sécurité de la gestion des données.

- L'association de différents niveaux de sécurité aux applications et l'utilisation de moyens de chiffrement différents (typiquement algorithmes, longueurs de clés) selon le niveau de sécurité associé

permettent de proportionner le coût de mise en oeuvre (temps d'exécution notamment) à l'objectif recherché en matière de sécurité.

A titre d'exemple non limitatif, il pourra être justifié de réserver les moyens cryptographiques les plus puissants (et les plus coûteux) pour la protection d'une unité de mémoire destinée à recevoir des clefs de chiffrement ou des droits d'accès.

- La combinaison du procédé selon l'invention à un mécanisme de protection physique (MMU) permet une protection à granularité plus fine. Par exemple, les applications peuvent être regroupées en plusieurs grandes catégories (éventuellement, et de manière non limitative, selon le niveau de confiance qu'on peut leur accorder, la première distinction naturelle pouvant être entre applications des utilisateurs et applications du système d'exploitation), chaque catégorie étant protégée des autres par le mécanisme physique et les applications étant protégées entre elles par le procédé de confinement logiciel selon l'invention.

REVENDICATIONS

1. Procédé de sécurisation par confinement logiciel d'un système informatique qui exécute des codes manipulant des données, faisant intervenir :

- au moins un gestionnaire de mémoire gérant des unités d'allocation mémoire qui peuvent être typiquement une page de taille fixe ou un bloc de taille variable,
- au moins des possesseurs et des demandeurs d'unités d'allocation mémoire pouvant être typiquement une application de l'utilisateur du système d'exploitation du système informatique ou le système d'exploitation lui-même,

caractérisé en ce qu'il comprend les étapes suivantes :

- une allocation de mémoire réalisée par le gestionnaire de mémoire à la demande d'un autre composant du système d'exploitation qui transmet audit gestionnaire de mémoire l'identité du demandeur ;
- un contrôle par le susdit gestionnaire de mémoire de l'ensemble des unités d'allocation, chacune étant associée à un possesseur de l'unité d'allocation mémoire ;
- un chiffrement des données de chaque possesseur à l'aide d'une clé associée à ce possesseur ;
- une vérification par le gestionnaire de mémoire, pour chaque demande d'accès à une unité d'allocation mémoire, de l'identité du demandeur ; si cette identité n'est pas identique à celle du possesseur de ladite unité d'allocation mémoire, alors l'accès à l'unité d'allocation mémoire est refusé par le gestionnaire de mémoire ;
- une réalisation par le gestionnaire de mémoire du chiffrement (dans le cas d'une demande d'écriture) ou du déchiffrement (dans le cas d'une demande de lecture) des données concernées avec la clé associée au possesseur, cette clé étant au moins recalculée par le gestionnaire de mémoire.

2. Procédé selon la revendication 1, caractérisé en ce que l'unité d'allocation est la page, et que le gestionnaire de mémoire, lorsqu'il reçoit une demande d'allocation d'un bloc pour le compte d'un possesseur d'unité d'allocation mémoire, recherche d'abord une page ayant le même possesseur de façon à ce que tous les blocs alloués par ledit possesseur se trouvent regroupés dans une ou plusieurs pages dédiées.

3. Procédé selon la revendication 1, caractérisé en ce que la transmission de l'identité du demandeur se fait soit par la gestion d'un contexte courant, soit par le passage de paramètres aux fonctions du gestionnaire de mémoire.

4. Procédé selon la revendication 1, caractérisé en ce que le gestionnaire de mémoire calcule dynamiquement la clé d'un possesseur à partir d'un secret associé audit possesseur et d'une clé dite "maître" à laquelle seul le gestionnaire de mémoire a accès.

5. Procédé selon la revendication 1, caractérisé en ce que le gestionnaire de mémoire associe une clé à chaque ensemble possesseur et unité d'allocation mémoire au lieu d'associer une clé unique à chaque possesseur.

6. Procédé selon la revendication 1, caractérisé en ce que le gestionnaire de mémoire intègre dans chaque unité d'allocation mémoire une zone permettant d'en vérifier l'intégrité.

7. Procédé selon la revendication 1, caractérisé en ce qu'il associe différents niveaux de sécurité aux applications et utilise des moyens de chiffrement différents selon le niveau de sécurité associé.

8. Procédé selon la revendication 1, caractérisé en ce qu'il est combiné à un mécanisme de protection physique.

9. Procédé selon la revendication 1, caractérisé en ce qu'il est implémenté sur un système embarqué tel un terminal du type téléphone portatif, un terminal de paiement bancaire, un terminal de paiement portatif, un assistant digital ou "PDA", une carte à puce.